(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-204134
(P2005-204134A)
(43)公開日　平成17年7月28日(2005.7.28)

(51) Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/10	H04L	9/00	621A	5B017
G06F 12/14	G06F	12/14	310Z	5J104
G06F 17/60	G06F	17/60	242	
G09C 1/00	G09C	1/00	660A	

審査請求 未請求　請求項の数 8　OL　（全 10 頁）

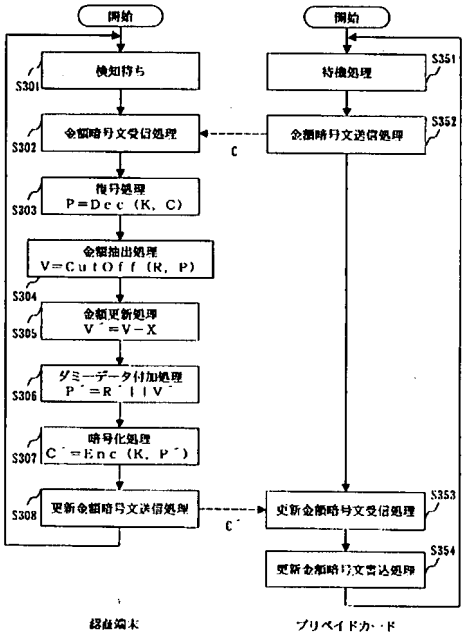
(21)出願番号　特願2004-9134 (P2004-9134)
(22)出願日　平成16年1月16日 (2004.1.16)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(74)代理人　100099461
弁理士　溝井　章司
(74)代理人　100111800
弁理士　竹内　三明
(72)発明者　三澤　学
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　山田　敬喜
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

Fターム(参考)　5B017 AA02 BA07 CA14
5J104 AA12 NA35 NA42 PA10 PA12

(54)【発明の名称】耐タンパ暗号システム及びメモリ装置及び認証端末及び及びプログラム

(57)【要約】
【課題】　プリペイドカード等のメモリの更新技術に係り、サイドチャネルアタックによる不正解析を困難にし、メモリ記憶値の改ざんを防止することを課題とする。
【解決手段】　認証装置は、メモリ装置から受信した管理データ暗号文を復号し（Ｓ３０３）、そこから先頭の乱数を除去して、金額を抽出する（Ｓ３０４）。そして、消費金額を差し引いて、残高となる更新金額を算出する（Ｓ３０５）。更新金額の先頭にダミーデータとして乱数を付加したのちに（Ｓ３０６）、これを暗号化する（Ｓ３０７）。その暗号結果を、プリペイドカードに書き込む。また、暗号ブロック連鎖モードの暗号方式を採用することも有効である。
【選択図】　図３



【特許請求の範囲】
【請求項１】
ダミーデータが付加された管理データを秘匿状態に変換した管理データ暗号文を外部より受信する管理データ暗号文受信部と、
受信した前記管理データ暗号文を復号する復号部と、
復号結果から前記ダミーデータを除いて、前記管理データを抽出する管理データ抽出部と、
抽出した前記管理データを更新して更新管理データを生成する管理データ更新部と、
前記更新管理データに新たなダミーデータを付加するダミーデータ付加部と、
前記新たなダミーデータが付加された更新管理データを暗号化して更新管理データ暗号文を生成する暗号化部と、
前記更新管理データ暗号文を外部へ送信する更新管理データ暗号文送信部と
を有することを特徴とする認証端末。
【請求項２】
ダミーデータが付加された管理データを秘匿状態に変換した管理データ暗号文を保持するメモリ装置であって、
前記管理データ暗号文を記憶する管理データ暗号記憶部と、
該管理データ暗号記憶部で記憶している前記管理データ暗号文を外部へ送信する管理データ暗号文送信部と、
外部から新たなダミーデータが付加された更新された管理データが秘匿状態に変換された更新管理データ暗号文を受信する更新管理データ暗号文受信部と、
受信した前記更新管理データ暗号文を前記管理データ暗号記憶部に書き込む更新管理データ暗号文書込部と
を有することを特徴とするメモリ装置。
【請求項３】
メモリ装置は、プリペイドカード、ＲＦＩＤ（電波方式認識）カード、あるいはＩＣカードのいずれか、または不揮発メモリを有した端末であって、
管理データは、金額、量、回数、または度数であることを特徴とする請求項２記載のメモリ装置。
【請求項４】
ダミーデータが付加された管理データを秘匿状態に変換した管理データ暗号文を保持するメモリ装置と、前記管理データを更新する認証端末とからなり、互いに通信可能な耐タンパ暗号システムであって、
前記メモリ装置は、前記管理データ暗号文を記憶する管理データ暗号記憶部と、
該管理データ暗号記憶部で記憶している前記管理データ暗号文を前記認証端末へ送信する管理データ暗号文送信部とを有し、
前記認証端末は、前記メモリ装置から前記管理データ暗号文を受信する管理データ暗号文受信部と、
受信した前記管理データ暗号文を復号する復号部と、
復号結果から前記ダミーデータを除いて、前記管理データを抽出する管理データ抽出部と、
抽出した前記管理データを更新して更新管理データを生成する管理データ更新部と、
前記更新管理データに新たなダミーデータを付加するダミーデータ付加部と、
前記新たなダミーデータが付加された更新管理データを暗号化して更新管理データ暗号文を生成する暗号化部と、
前記更新管理データ暗号文を前記メモリ装置へ送信する更新管理データ暗号文送信部とを有し、
前記メモリ装置は、更に、前記認証端末から前記更新管理データ暗号文を受信する更新管理データ暗号文受信部と、
受信した前記更新管理データ暗号文を前記管理データ暗号記憶部に書きこむ更新管理デ

ータ暗号文書込部と
を有することを特徴とする耐タンパ暗号システム。
【請求項５】
メモリ装置は、プリペイドカード、R.ＦＩＤ（電波方式認識）カード、あるいはＩＣカードのいずれか、または不揮発メモリを有した端末であって、
管理データは、金額、量、回数、または度数であることを特徴とする請求項４記載の耐タンパ暗号システム。
【請求項６】
ダミーデータ付加部は、乱数を取得し、取得した乱数をダミーデータとして、更新管理データの先頭に付加し、
管理データ抽出部は、復号した平文から先頭のダミーデータを除いて、管理データを抽出することを特徴とする請求項４記載の耐タンパ暗号システム。
【請求項７】
暗号化部は、暗号ブロック連鎖モードの暗号化を行い、
復号部は、暗号ブロック連鎖モードの復号を行うことを特徴とする請求項４記載の耐タンパ暗号システム。
【請求項８】
管理データを秘匿状態に変換した管理データ暗号文を保持するメモリ装置と通信して、管理データを更新する認証装置となるコンピュータに、
メモリ装置から前記管理データ暗号文を受信する手順と、
受信した前記管理データ暗号文を復号する手順と、
復号した平文からダミーデータを除いて、管理データを抽出する手順と、
抽出した管理データを更新して更新管理データを生成する手順と、
更新管理データにダミーデータを付加する手順と、
ダミーデータを付加して得られた平文を、暗号化する手順と、
暗号の結果として得られた更新管理データ暗号文をメモリ装置へ送信する手順とを実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、プリペイドカードやＲＦＩＤ（Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ－Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ：電波方式認識）やＩＣカード、不揮発メモリを有した端末等のメモリの更新技術に係り、サイドチャネルアタックによる不正解析を困難にし、メモリ記憶値の改ざんを防止する技術に関する。
【背景技術】
【０００２】
本発明は、例えば、プリペイドカードやＲＦＩＤやＩＣカード、不揮発メモリを有した端末のように、サービスを提供する際にメモリに書き込まれている残高から使用額を減算し、その残高をカード等に書き込む方式等に関する。
【０００３】
残高をそのままカードに書き込むと、メモリのリーダライタや通信部分を擬似する装置があれば簡単にカードを偽造することが可能である。その為、暗号を用いて、残高を暗号化して書き込むことにより改ざんを防止している。
【０００４】
図８は、従来の処理フローを示す図である。認証端末１で、プリペイドカード２を検知すると、プリペイドカード２から暗号化されている金額を読み込む（Ｓ８０２）。そして、復号してから（Ｓ８０３）、金額等を更新し（Ｓ８０４）、その後暗号化して（Ｓ８０５）、プリペイドカード２に書き込む（Ｓ８０６）ように動作している。
【０００５】
しかし認証端末に対してサイドチャネルアタックができるような場合には、これだけで

は安全といえない。残高を暗号化する際の消費電力や電磁波等を観測し、サイドチャネルアタックによって暗号の秘密鍵を解析される可能性がある。

【発明の開示】

【発明が解決しようとする課題】

【０００６】

本発明は、上記した従来技術の欠点を除くためになされたものであって、その目的とするところは、プリペイドカード等のメモリの更新技術に係り、サイドチャネルアタックによる不正解析を困難にし、メモリ記憶値の改ざんを防止することである。

【課題を解決するための手段】

【０００７】

本発明に係る認証端末は、

ダミーデータが付加された管理データを秘匿状態に変換した管理データ暗号文を外部より受信する管理データ暗号文受信部と、

受信した前記管理データ暗号文を復号する復号部と、

復号結果から前記ダミーデータを除いて、前記管理データを抽出する管理データ抽出部と、

抽出した前記管理データを更新して更新管理データを生成する管理データ更新部と、

前記更新管理データに新たなダミーデータを付加するダミーデータ付加部と、

前記新たなダミーデータが付加された更新管理データを暗号化して更新管理データ暗号文を生成する暗号化部と、

前記更新管理データ暗号文を外部へ送信する更新管理データ暗号文送信部と

を有することを特徴とする。

【発明の効果】

【０００８】

本発明においては、金額である平文に乱数等のダミーデータ付加して暗号化するので、サイドチャネルアタックによる不正解析を困難にし、メモリ記憶値の改ざんを防止することができる。その他の効果として、同じ金額（量・回数・度数）を書いたとしても乱数等のダミーデータによって書き込む暗号文は毎回異なり、金額（量・回数・度数）を予想できないという効果もある。

【発明を実施するための最良の形態】

【０００９】

実施の形態１.

以下本発明を図面に示す実施例に基づいて説明する。図１は、想定環境を示す図である。この例では、プリペイドカードと、更新する認証端末を例としているが、更新対象である管理データ（特に、度数、回数などの数値の適用が多い）を、メモリに記憶し、その値を第三者の読み取り、改ざんから防御するシステムに適用可能である。例えば、ＲＦＩＤやＩＣカード、不揮発メモリを有した端末等にも適用可能である。

【００１０】

本発明では、サイドチャネルアタックの対策として、暗号化する際に平文の先頭にダミーデータ（例えば、乱数）を挿入することを特徴とする。

【００１１】

まず、構成について説明する。図２は、モジュール構成を示す図である。認証端末１は、金額暗号文受信部１０１、復号部１０２、金額抽出部１０３、金額更新部１０４、ダミーデータ付加部１０５、暗号化部１０６、及び更新金額暗号文送信部１０７を有している。プリペイドカード２は、金額暗号文記憶部２０１、金額暗号文送信部２０２、更新金額暗号文受信部２０３、及び更新金額暗号文書込部２０４を有している。

【００１２】

次に、処理について説明する。図３は、処理フローを示す図である。認証端末１は、プリペイドカード２を検知すると（Ｓ３０１）、金額暗号文受信部１０１で、プリペイドカード２の金額暗号文送信部２０２から送信される金額暗号文（金額を暗号化したデータ）

を受信する（Ｓ３０２）。

【００１３】

そして、復号部１０２でこれを復号処理する（Ｓ３０３）。このとき、内部で予め秘密状態で記憶している暗号鍵を用いる。

【００１４】

そして、金額抽出部１０３で、金額抽出処理（Ｓ３０４）する。復号により得られる平文Ｐからダミーデータを除去して、金額Ｖを抽出する。例えば、データの先頭部分ｗのダミーデータをＮＵＬＬにして、後の金額部分のみが有効なデータに書き換える。尚、図中で、ＣｕｔＯｆｆ（Ｘ，Ｙ）は、ＹからＸを削除する関数を意味している。

【００１５】

次に、金額更新部１０４で、金額更新処理（Ｓ３０５）する。金額Ｖから支払い金額Ｘを引いて、残額Ｖ´を得る。残額Ｖ´が、更新される金額となる。

【００１６】

ダミーデータ付加部１０５で、ダミーデータ付加処理（Ｓ３０６）する。この処理で、更新金額Ｖ´に、ダミーデータ（例えば、乱数）を付加する。例えば、更新金額Ｖ´の先頭に、ダミーデータを付加する。尚、図中で、Ｘ｜｜Ｙは、ＸとＹを連結する処理を示している。乱数のように、都度異なる値を用いることが有効である。

【００１７】

暗号化部１０６で、ダミーデータが付加された更新金額を平文Ｐ´として、暗号化処理（Ｓ３０７）する。

【００１８】

こうして、暗号化された更新金額の暗号文Ｃ´を更新金額暗号文送信部１０７からプリペイドカード２に送信する（Ｓ３０８）。

【００１９】

プリペイドカード２では、これを更新金額暗号文受信部２０３で受信（Ｓ３５３）し、更新金額暗号文書込部２０４は、受信した更新金額暗号文Ｃ´で、金額暗号文記憶部２０１の値を更新する（Ｓ３５４）。

【００２０】

このように毎回異なる乱数から暗号化を始めることになり、暗号化途中での値を想定させないようにできる。従って、ＤＰＡ（Ｄｉｆｆｅｒｅｎｔｉａｌ Ｐｏｗｅｒ Ａｎａｌｙｓｉｓ）等によるサイドチャネルアタックが困難になる。

【００２１】

実施の形態２．

本発明は、上述の例以外にも、部分的に乱数を挿入しても、復号するときにその挿入した乱数の値を知らなくても復号できる方式（例えば、共通鍵ブロック暗号のＣＢＣモードや公開鍵暗号）に適用できる。

【００２２】

本実施の形態では、暗号ブロック連鎖（ＣＢＣ：Ｃｉｐｈｅｒ Ｂｌｏｃｋ Ｃｈａｉｎｉｎｇ）モードの暗号化と復号を用いる形態を説明する。

【００２３】

まず、暗号化について説明する。実施の形態１のダミーデータ付加部１０５と暗号化部１０６の処理に対応する。図４は、ＣＢＣモードに適用した場合の暗号化に係るブロックを示す図である。図５は、ＣＢＣモードに適用した場合の暗号化に係る処理フローを示す図である。これらの図を用いて、処理を説明する。

【００２４】

暗号化される平文Ｐ´は、乱数Ｒと、Ｍ１，Ｍ２，…の実データのブロックから構成されている。そして、この先頭ブロックから順に以下の処理を繰り返す（Ｓ５０１）。

【００２５】

先頭から順に、平文データのブロックを取得する（Ｓ５０２）。最初は、Ｒを得る。二回目以降は、Ｍ１，Ｍ２，…の順に取得する。これは、論理演算（４０１，４０２，４０

3，…）の一方の入力となる。

【００２６】

他の入力データとなる入力側パラメータも特定する（Ｓ５０３）。最初は、乱数ＩＶ（ダミーデータに相当）を用いる。二回目以降は、前回の暗号結果（順に、Ｃ０´，Ｃ１´，…）を用いる。

【００２７】

そして、これらの入力側論理演算（Ｓ５０４）を行う。この例は、排他的論理和（ＸＯＲ）を求めている。図４の４０１，４０２，４０３に示す処理である。

【００２８】

演算結果（最初は、Ｒ´、順にＭ１´，Ｍ２´，…）を内部で記憶している暗号鍵ｕｋｅｙで暗号化する（Ｓ５０５）。その結果として、順にＣ０´，Ｃ１´，Ｃ２´，…を得る。

【００２９】

暗号結果と、復号側と共通して用いる乱数ＦＶを入力として、出力側論理演算する（Ｓ５０６）。この例は、排他的論理和（ＸＯＲ）を求めている。図４の４２１，４２２，４２３に示す処理である。

【００３０】

そして、演算結果を暗号データのブロックとして順に記憶する（Ｓ５０７）。順に、Ｃ０，Ｃ１，Ｃ２，…となる。

【００３１】

すべてのブロックを処理した時点で終了する（Ｓ５０８）。

【００３２】

続いて、復号について説明する。実施の形態１の復号部１０２と金額抽出部１０３の処理に対応する。図６は、ＣＢＣモードに適用した場合の復号に係るブロックを示す図である。図７は、ＣＢＣモードに適用した場合の復号に係る処理フローを示す図である。

【００３３】

暗号データは、Ｃ０，Ｃ１，Ｃ２，…のブロックから構成されている。そして、この先頭ブロックから順に以下の処理を繰り返す（Ｓ７０１）。

【００３４】

先頭から順に、暗号データのブロックを取得する（Ｓ７０２）。これは、論理演算（６０１，６０２，６０３，…）の一方の入力となる。

【００３５】

他方の入力データとして、暗号側と共通して用いる乱数ＦＶを用いて、入力側論理演算（Ｓ７０３）を行う。この例は、排他的論理和（ＸＯＲ）を求めている。図６の６０１，６０２，６０３に示す処理である。

【００３６】

演算結果（最初は、Ｃ０´，Ｃ１´，Ｃ２´，…）を内部で記憶している暗号鍵ｕｋｅｙで復号する（Ｓ７０４）。その結果として、順にＲ´，Ｍ１´，Ｍ２´，…を得る。復号結果は、出力側論理演算の一方の入力となる。

【００３７】

他の入力となる出力側パラメータを特定する（Ｓ７０５）。最初は、乱数ＩＶ（ダミーデータに相当）を用いる。二回目以降は、前回の復号入力データ（順に、Ｃ０´，Ｃ１´，…）を用いる。

【００３８】

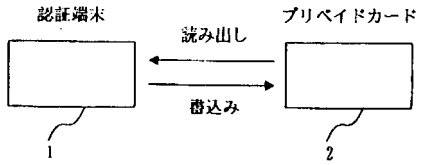
そして、これらの出力側論理演算（Ｓ７０６）を行う。この例は、排他的論理和（ＸＯＲ）を求めている。図６の６１１，６１２，６１３に示す処理である。

【００３９】

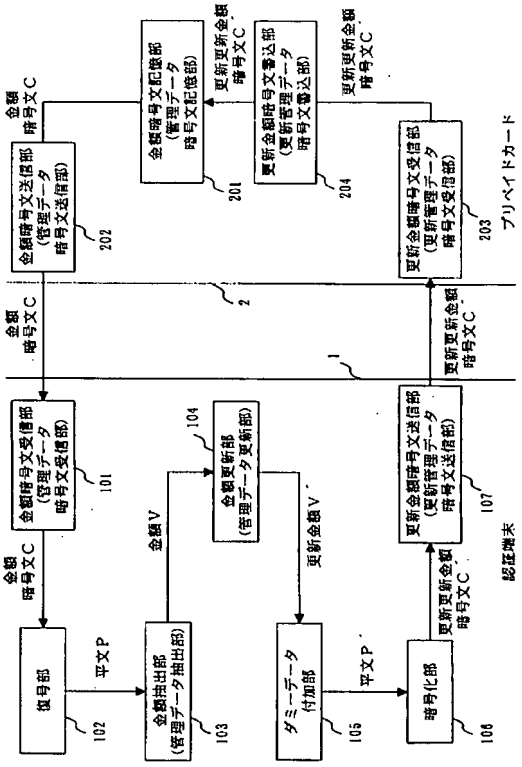
演算結果を平文データのブロックとして順に記憶する（Ｓ７０７）。順に、Ｒ，Ｍ１，Ｍ２，…となる。但し、ダミーデータである乱数Ｒは、無視して、Ｍ１以降のブロックを用いる。

【００４０】
乱数Ｒは１ブロック分でなくても構わない。２ブロック分でも、１ブロックより少なくても本発明に適用可能である。つまり、乱数がどの部分であるかということさえわかっていればよい。また乱数を挿入するブロックも１ブロック目でなくても、２ブロック目や３ブロック目でも構わない。また、ＲＳＡなどの共通鍵暗号方式の場合には、ブロックは関係なくなり、乱数もどの位置に入れても、乱数の位置さえわかっていればよい。これは、実施の形態１についても同様である。
【００４１】
すべてのブロックを処理した時点で終了する（Ｓ７０８）。
【００４２】
認証端末１は、コンピュータであり、各要素はプログラムにより処理を実行することができる。また、プログラムを記憶媒体に記憶させ、記憶媒体からコンピュータに読み取られるようにすることができる。
【００４３】
図９は、認証端末のハードウエア構成例を示す図である。バスに、演算装置９０１、データ記憶装置９０２、メモリ９０３、通信インターフェース９０４が接続されている。データ記憶装置９０２は、例えばＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）やハードディスクである。メモリ９０３は、通常ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）である。
【００４４】
プログラムは、通常データ記憶装置９０２に記憶されており、メモリ４０３にロードされた状態で、順次演算装置９０１に読み込まれ処理を行う。金額等のデータの受信や送信は、通信インターフェース９０４により行う。
【図面の簡単な説明】
【００４５】
【図１】想定環境を示す図である。
【図２】モジュール構成を示す図である。
【図３】処理フローを示す図である。
【図４】ＣＢＣモードに適用した場合の暗号化に係るブロックを示す図である。
【図５】ＣＢＣモードに適用した場合の暗号化に係る処理フローを示す図である。
【図６】ＣＢＣモードに適用した場合の復号に係るブロックを示す図である。
【図７】ＣＢＣモードに適用した場合の復号に係る処理フローを示す図である。
【図８】従来の処理フローを示す図である。
【図９】認証端末のハードウエア構成例を示す図である。
【符号の説明】
【００４６】
１　認証端末、２　プリペイドカード、１０１　金額暗号文受信部、１０２　復号部、１０３　金額抽出部、１０４　金額更新部、１０５　ダミーデータ付加部、１０６　暗号化部、１０７　更新金額暗号文送信部、２０１　金額暗号文記憶部、２０２　金額暗号文送信部、２０３　更新金額暗号文受信部、２０４　更新金額暗号文書込部。

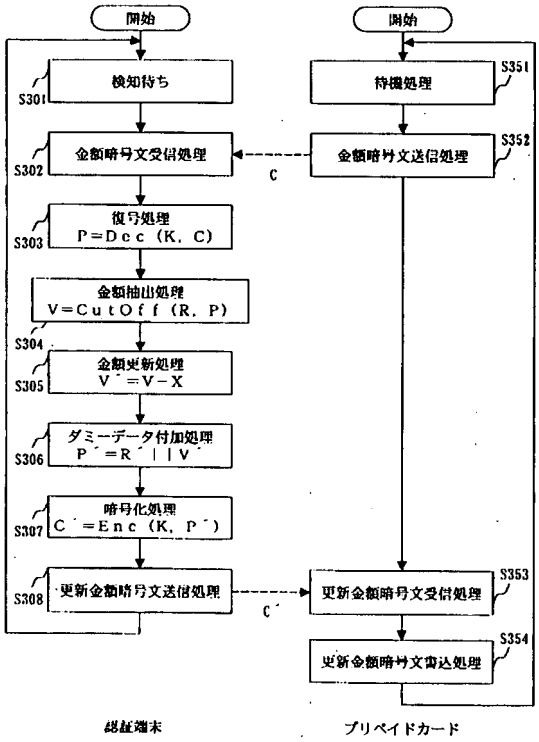
【図１】


認証端末
読み出し
書込み
プリペイドカード
1
2

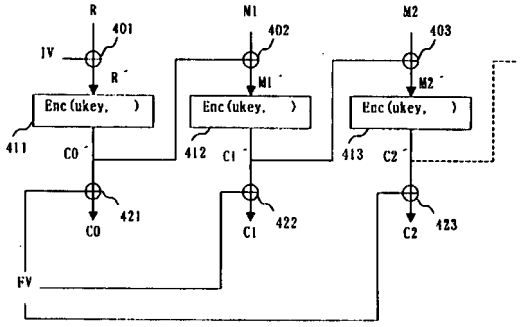
【図２】


金額暗号文送信部（管理データ暗号文送信部）
202
金額暗号文記憶部（管理データ暗号文記憶部）
201
更新金額暗号文書込部（更新管理データ暗号文書込部）
204
更新金額暗号文受信部（更新管理データ暗号文受信部）
203
プリペイドカード
金額暗号文C
更新更新金額暗号文C´
2
1
金額暗号文受信部（管理データ暗号文受信部）
101
金額更新部（管理データ更新部）
104
更新金額暗号文送信部（更新管理データ暗号文送信部）
107
認証端末
金額V
更新金額V´
復号部
102
平文P
金額抽出部（管理データ抽出部）
103
ダミーデータ付加部
105
平文P´
暗号化部
106
更新更新金額暗号文C´

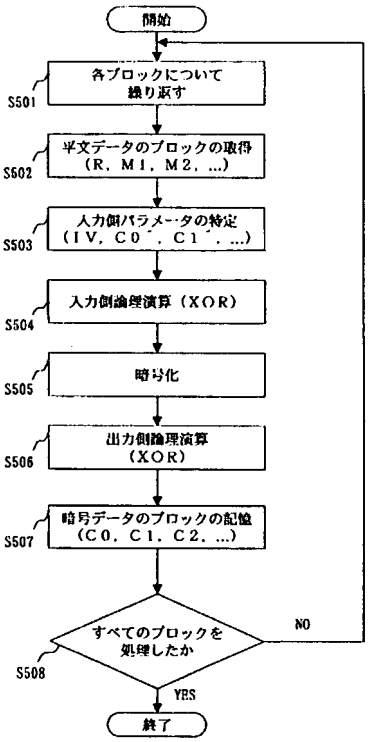
【図３】


開始
検知待ち
S301
金額暗号文受信処理
S302
C
復号処理
P=Dec（K，C）
S303
金額抽出処理
V=CutOff（R，P）
S304
金額更新処理
V´=V−X
S305
ダミーデータ付加処理
P´=R´||V´
S306
暗号化処理
C´=Enc（K，P´）
S307
更新金額暗号文送信処理
S308
C´
開始
待機処理
S351
金額暗号文送信処理
S352
更新金額暗号文受信処理
S353
更新金額暗号文書込処理
S354
認証端末
プリペイドカード

【図４】

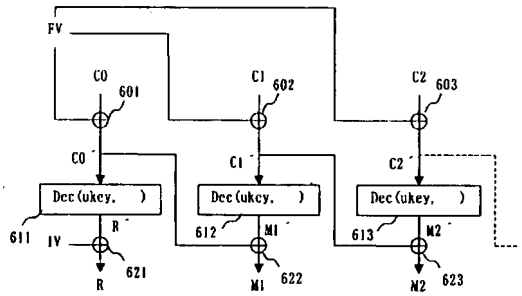

R
401
IV
R´
Enc(ukey,)
411
C0´
C0
421
M1
402
M1´
Enc(ukey,)
412
C1´
C1
422
M2
403
M2´
Enc(ukey,)
413
C2´
C2
423
FV

【図５】

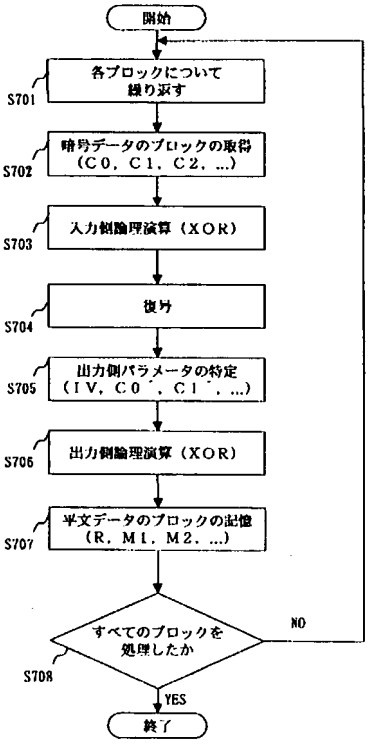


<CBCモードの暗号化>

【図６】

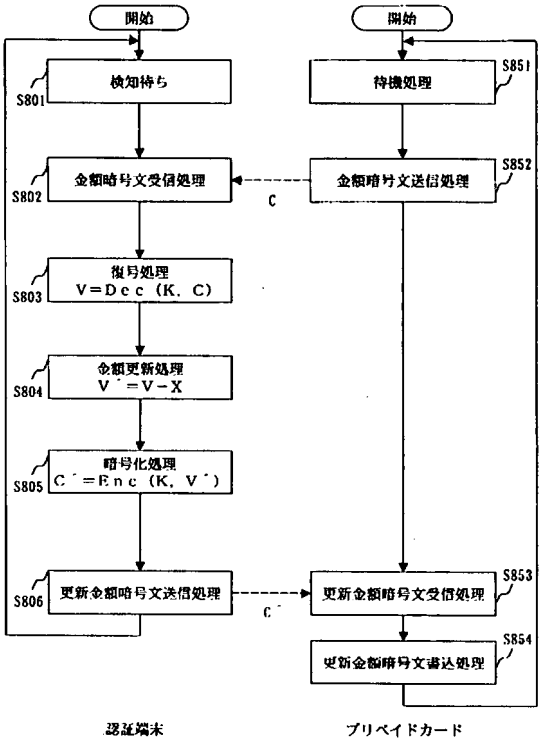


【図７】



<CBCモードの復号>

【図８】



【図９】